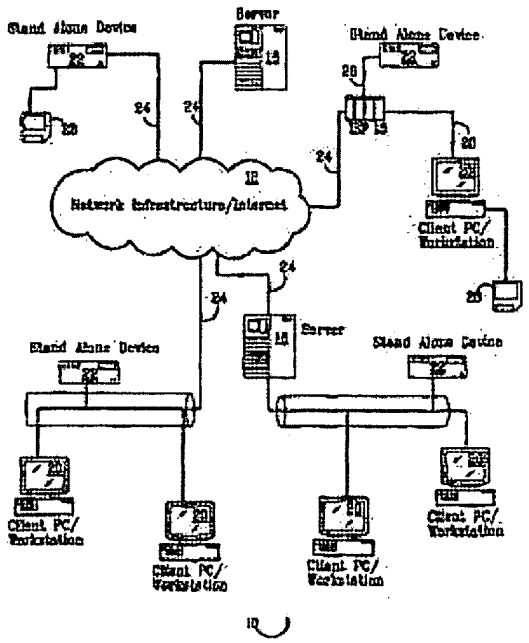
# System for keying protected electronic data to particular media to prevent unauthorized copying using asymmetric encryption and a unique identifier of the media

**Publication number:** TW484292 (B)
**Publication date:** 2002-04-21
**Inventor(s):** KUPKA MICHAEL S [US]; HAWKINS MICHAEL L [US]; THOMAS TRENT M [US]
**Applicant(s):** IOMEGA CORP [US]
**Classification:**
**- international:** ***G06F1/00; G06F21/00; H04L29/06;*** **G06F1/00; G06F21/00; H04L29/06;** (IPC1-7): H04L9/00
**- European:** H04L29/06S4B2; G06F21/00N7D
**Application number:** TW19990119840 19991115
**Priority number(s):** US19980191666 19981113

**Also published as:**
WO0030319 (A1)

Abstract of **TW 484292 (B)**

An apparatus and method of electronically distributing electronic data from a server to a client device via a network infrastructure. The method and apparatus utilizes asymmetric encryption (e.g., public key encryption) to transfer data from a server to a client device. Once the data is received by the client device, it is written to a destination media such that it cannot be accessed from any other piece of media. A unique identifier of the media, which is embedded onto the media during the manufacturing process is used to prevent access from other pieces of media. The downloaded data may also be associated to the media by a compound key that includes the unique identifier of the media, a vendor identifier and a user identifier.; The method and system establishes a connection between the client device and the server via the network infrastructure; transmits, via the network infrastructure, the public key; encrypts, at the server, the key to the protected electronic data to be communicated to the client; communicates, via the network infrastructure, the electronic data to the client device, wherein the electronic data is in an encrypted format; decrypts the electronic data in accordance with the key to protected data; and writes, at the client device, the electronic data to the one piece of media, such that the information may be accessed for use from only the one piece of destination media. The electronic data is encrypted and written to the media using either the aforementioned unique identifier or compound key.



公告本

| | |
|---|---|
| 申請日期 | 88.11.15 |
| 案號 | 88119840 |
| 類別 | H04L 9/00 |

（以上各欄由本局填註）

A4
C4

484292

# 發明 新型 專利說明書

| | | |
|---|---|---|
| 一、發明新型名稱 | 中文 | 使用非對稱加密及媒體獨一識別子將保護之電子資料鎖入特別媒體以防止非授權拷貝之系統 |
| | 英文 | SYSTEM FOR KEYING PROTECTED ELECTRONIC DATA TO PARTICULAR MEDIA TO PREVENT UNAUTHORIZED COPYING USING ASYMMETRIC ENCRYPTION AND A UNIQUE IDENTIFIER OF THE MEDIA |
| 二、發明創作人 | 姓名 | 1.麥可 S.古布卡<br>2.麥可 L.霍金斯<br>3.川特 M.湯馬士 |
| | 國籍 | 美 國 |
| | 住、居所 | 1.美國,德州 75961,納可格達屈,坎溪路 4521 號<br>2.美國,德州 75961,納可格達屈,普魯依特山路 1324 號<br>3.美國,猶他州 84403,奧格登,山邊廣場 1758 號 |
| 三、申請人 | 姓名（名稱） | 伊歐美卡公司 |
| | 國籍 | 美 國 |
| | 住、居所（事務所） | 美國,猶他州 84067,洛伊市,西伊歐美卡路 1821 號 |
| | 代表人姓名 | 查洛特 L.米勒 |

（由本局填寫）

| | |
|---|---|
| 承辦人代碼： | |
| 大　　類： | |
| ＩＰＣ分類： | |

A6
B6

本案已向：

| 國（地區） | 申請專利，申請日期： | 案號： | ，☑有 □無主張優先權 |
|---|---|---|---|
| 美 | 1998.11.13 | 09/191,666 | |

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

A5
B5

四、中文發明摘要（發明之名稱：　　）

使用非對稱加密及媒體獨一識別子將保護之電子資料鎖入特別媒體以防止非授權拷貝之系統

一種用於經由網路基礎結構而分配電子資料之系統與方法。該方法以及裝置係利用非對稱式加密(例如公共鑰匙加密)以將資料從一伺服器轉移至一用戶裝置。一旦用戶裝置接收到該資料，係將之寫入一目的媒體以致無法從任何其他塊媒體接達之。係利用該媒體之唯一的識別子來防止從其他塊的媒體接達，該唯一的識別子係在製造過程中埋入該媒體。所下載之資料係可藉由一複合鑰匙而與該媒體相關聯，該複合鑰匙係包括媒體之唯一的識別子，販售者

英文發明摘要（發明之名稱：　　）

**SYSTEM FOR KEYING PROTECTED ELECTRONIC DATA TO PARTICULAR MEDIA TO PREVENT UNAUTHORIZED COPYING USING ASYMMETRIC ENCRYPTION AND A UNIQUE IDENTIFIER OF THE MEDIA**

An apparatus and method of electronically distributing electronic data from a server to a client device via a network infrastructure. The method and apparatus utilizes asymmetric encryption (e.g., public key encryption) to transfer data from a server to a client device. Once the data is received by the client device, it is written to a destination media such that it cannot be accessed from any other piece of media. A unique identifier of the media, which is embedded onto the media during the manufacturing process is used to prevent access from other pieces of media. The downloaded data may also be associated to the media by a compound key that includes the unique identifier of the media, a vendor identifier and a user

A5
B5

四、中文發明摘要（發明之名稱：　　）

識別子以及使用者識別子。該方法以及系統係經由該網路基礎結構建立該用戶裝置與該伺服器之間的連接；經由該網路基礎結構傳送該公共鑰匙至該伺服器；在該伺服器將欲通訊至用戶之該用於該受保護之電子資料之鑰匙加密；經由該網路基礎結構將該電子資料通訊至該用戶裝置，其中該電子資料係在一經加密之格式；根據該用於該受保護之資料之鑰匙將該電子資料解密；以及在用戶裝置將該電子資料寫入該一塊之媒體，以致該資訊僅可從該一塊之該目的媒體接達以便使用。該電子資料係利用前述之唯一的識別子或是複合鑰匙而加密並且寫入該媒體。

英文發明摘要（發明之名稱：　　）

identifier. The method and system establishes a connection between the client device and the server via the network infrastructure; transmits, via the network infrastructure, the public key; encrypts, at the server, the key to the protected electronic data to be communicated to the client; communicates, via the network infrastructure, the electronic data to the client device, wherein the electronic data is in an encrypted format; decrypts the electronic data in accordance with the key to protected data; and writes, at the client device, the electronic data to the one piece of media, such that the information may be accessed for use from only the one piece of destination media. The electronic data is encrypted and written to the media using either the aforementioned unique identifier or compound key.

五、發明說明（ 1 ）

相關申請案之交互參考：

本發明係於 1998 年四月 17 日提出申請，標題爲「將保護之電子資料鎖入特別媒體以防止非授權拷貝之系統」之美國專利申請案序號第 09/061493 號的部分接續案。

發明領域：

本發明係有關於藉由使電子資料與儲存媒體之特定一塊相關聯而防止非授權拷貝。明確而言，本發明係有關於一種遠程資料遞送系統，其中欲加以保護之電子資料係以一種安全的方式而遞送至一區域機器，該區域機器係儲存該受保護之電子資料並且永久性地使該受保護之電子資料與儲存媒體之一特定塊相關，其乃係依據至少利用該媒體之一個唯一的識別子之複合鑰匙。

發明背景：

對於著作權以及保護形式之數位儲存資料的保護已經成爲此種資料之所有者歷來之主要關切事情。明確而言，電腦軟體，音樂以及影片之著作權侵害已經成爲大受矚目之事件並且持續如此，因爲幾乎無法阻止。雖然已經有由軟體，音樂以及影片業者所作之許多先前之嘗試以減少著作權侵害，但是每一種都只達到有限的成功。

作爲對打擊著作權侵害之部分努力，軟體販售者在販賣時係已經許可軟體而非轉移所有權。當購買軟體時，購買者係成爲一個被認可的使用者(被特許者)而非所有者。在大多數許可協定之下的軟體拷貝一般係限制於只有用於備份目的之一份拷貝，以便合法地限制無限的拷貝。此外

五、發明說明（２）

，軟體許可一般係准許在單一電腦上使用或是僅由一個使用者在任何時間來使用該軟體的權利。

軟體販售者亦經常係藉由對其軟體做拷貝保護來打擊軟體盜版。雖然此種嘗試在某種程度上是有效的，但是卻因爲使用者無法製作備份拷貝而告失敗。再者，在第一拷貝保護之電腦軟體在市場上不久，就有其他用來拷貝該拷貝軟體的程式供應。其他的著作權保護方法因而發展以試圖阻止盜版，但亦僅達到有限的成功。這些嘗試包括要求一主軟碟需插入電腦，或是在從電腦之硬碟機執行該軟體時，要求使用者鍵入包含在使用者手冊或許可協定的一個鑰匙或是其他資訊。其他的則是要求一硬體鑰匙出現在電腦的並列埠，當執行軟體時即讀取之。當光碟機(CD-ROM)成爲用於數位儲存以及軟體分配的標準媒體時，軟體販售者係得到暫時的舒緩，因爲應用成長如此之大，以致用於拷貝軟體的手段僅有在昂貴的可記錄式光碟上“燒錄”複製。然而，可記錄式光碟以及用於寫入可記錄式光碟之驅動器的價格大幅滑落，而著作權侵害者再度能夠製造受保護軟體之廉價的非法拷貝。

相較於軟體販售者，音樂以及影片工業有不同的關切焦點。這些工業特別關心著作權侵害者製作數位儲存之音樂以及影片的完美拷貝。雖然用於非商業目的之音樂以及影片的拷貝是容許的，此種拷貝過去以來係藉由錄放音機以及卡式錄放影機利用類比錄製技術而實行。類比重製造成隨著每一代而品質下降，反之數位拷貝係確實的並且不

五、發明說明（ 3 ）

會遭受傳真性的損失。應注意的是，可記錄式光碟以及用於寫入可記錄式光碟之驅動器的價格已經大幅滑落，而這些驅動器正可以輕易地將音樂記錄至光碟，一如其記錄軟體以及資料般。甚且，數位多用途碟片(DVD)的到來，現在可將完整長度之動畫記錄至一單一 DVD 碟片。結果，音樂以及影片工業亦有防止數位錄製作品之拷貝的增大的需求。

助長軟體販售者以及音樂和影片工業之關切的是數位時代來臨以及全球通訊的快速成長。在 1980 年代早期，當個人電腦處於其萌芽時期，而軟體販售者首度嘗試去保護他們的智慧財產權之時，即使有的話，也只有極少數大量分配管道。在同一時期，音樂以及影片工業於消費者階層全然爲類比。因此，盜版並不是主要的問題，因爲其係限制於小群的人或是機構。然而，隨著功能強大的電腦出現在每一個桌面上，以及音樂和影片發展進入數位模式，盜版成爲一個主要的要素，單是就軟體販售者而言，全世界一年就耗費四十億美元。相當明白的是，對於軟體開發者，音樂家，演藝人員以及其相關工業而言，經濟上的損失是極爲龐大的。

全球通訊擴展的根源在於網際網路的快速成長，其將盜版問題推至前線。如此項技藝中眾所週知者，『網際網路』一詞係在 1982 年首次使用以指使用傳輸控制協定/網際網路協定(TCP/IP)等協定之互相連接的網路的巨大集合。姑且不論在過去四年來得到大眾的認可，網際網路在

五、發明說明（ 4 ）

1960 年代晚期就已經存在，並且原始係設計爲廣域網路(WAN)，此種網路可在核子戰爭中存活。歷經 1970 以及 1980 年代，數目持續成長的小型網路發展並且經由網間連接器(gateway)連接至網際網路，作爲交換電子郵件的手段。在 1980 年代中期，可供使用的網際網路主機的數目有顯著的成長，並且自 1980 年代晚期之後，網際網路已經成指數成長。網際網路的成長係提供全世界的人們分享以及分配資訊的管道。因此現在盜版軟體，音樂以及影片之全球規模的大量分配的潛在性已存在。許多網際網路 Usenet 群聚以及在 Internet Relay Chat (IRC)上的通道係對於盜版檔案，音樂，以及影片的交易有所貢獻。助長盜版問題的是維持高評價並且深以其盜版成績爲傲的群體。盜版問題已經增加得如此嚴重以致有一個新名詞 “warez” 係用來表示盜版作品。網際網路現在係提供了合法銷售以及分配受保護之軟體，音樂以及影片的龐大潛力，此乃是因爲它的大小，速度以及對於消費者家庭的滲透力。然而，此等極佳的優點使得著作權侵害者可輕易地盜取花費數年來設計以及製造的專利軟體，並且在數小時內即可供應任何人，而取得不花分毫。

有鑒於以上所述者，需要有一種安全的方法以及裝置用於資料的電子分配，其可利用如網際網路等網路之廣泛分配，與此同時防止受保護的作品，資料以及應用之非授權以及非法拷貝。明確而言，需要有一種方法以及裝置，其係提供軟體，音樂以及影片之販售者一種在大型網路上

五、發明說明（ 5 ）

電子分配其作品以及應用之安全手段，同時確保其受保護之作品以及應用不會被拷貝以及侵害著作權。此種方法以及裝置亦可確保智慧財產權的所有者之權利受到保護，以及對於所有者其創作心血會得到適當的補償。

發明概述：

基於以上之觀點，本發明因而經由其一或多個方面及/或實施例而呈現以達成一或多個目的以及優點，如同以下所述及者。

根據本發明的一個方面，提供有一種經由一網路基礎結構電子分配電子資料至用戶裝置之方法。該方法以及裝置係利用一非對稱(例如公共鑰匙加密)以將資料從一伺服器轉移至一用戶裝置。一旦由用戶裝置接收到該資料之後，其係寫入一目的媒體以致其無法從任何其他塊媒體之接達。本發明之此特點係藉由利用該媒體之唯一的識別子而達成，該唯一的識別子係在製造過程中埋於該媒體。或者，經下載之資料可藉由一複合鑰匙而與該媒體相關聯，該複合鑰匙係包括該媒體之該唯一的識別子，販售者識別子，以及使用者識別子以使該電子資料與該一塊之媒體相關聯。該方法以及系統係包括建立用戶裝置與伺服器之間經由網路基礎結構之連接；經由該網路基礎結構傳送該公共鑰匙；在伺服器以該鑰匙將欲通訊至用戶的電子資料加密；經由該網路基礎結構將該電子資料通訊至用戶裝置，其中該電子資料係在一種加密之格式；根據加至該受保護之資料之鑰匙將該電子資料解密，以及在用戶裝置將該電子

五、發明說明（ 6 ）

資料寫入該一塊之媒體，以致此資訊僅可從該一塊之該目的媒體接達以供使用。該電子資料係利用前述之唯一的識別子或是複合鑰匙而加密並且寫至該媒體。

根據本發明之一特徵，將複合鑰匙傳送至伺服器係包括接達該一塊之目的媒體；從該一塊之目的媒體上的一預定位置讀取該唯一識別子；取得販售者資訊；取得使用者資訊；利用該唯一識別子，該販售者資訊，以及該使用者資訊，經由一預定運算而建立該複合鑰匙，以及將該複合鑰匙格式化成第一資料結構以用於通訊至該伺服器。該一塊之目的媒體上的該預定位置可爲一預定軌道。

本發明之其他特徵係如下所述。

圖式之簡單說明：

當連同所附圖式而觀賞時，將可更加明瞭先前所述之概述以及以下之較佳實施例之詳細說明。爲了闡示本發明的緣故，在該等圖式中顯示有目前較佳之實施例，其中在該等圖式之全部數個視圖中，相同的參考號碼係表示類似的部件，然而應明瞭本發明並不受限於所揭示之特定的方法與手段。在該等圖式中：

第一圖係一示範之電腦網路環境，本發明係可實施於其中；

第二圖係第一圖中所示之一用戶個人電腦/工作站之組件的方塊圖；

第三圖係第二圖中所示之一較佳媒體驅動器之組件的方塊圖；

五、發明說明（ 7 ）

第四圖係第一圖中所示之示範單機(stand alone)裝置之組件的方塊圖；

第五圖係顯示根據本發明之資料的電子分配中所實行之程序的流程圖；

第六圖係顯示實行於取得該媒體一唯一的識別子或是建立一複合鑰匙之程序的流程圖；以及

第七圖係用於本發明之示範的元檔案。

元件符號說明：

10 環境

12 網路基礎結構

14 區域網路

16 伺服器

18 ISP

20 用戶個人電腦/工作站

22 單機裝置

24 通訊鏈路

28 媒體

30 解密/解壓縮(解碼)裝置

34 USB/並列/串列埠控制器

36 ASIC/控制器

37 ROM

38 數位至類比轉換器

39 RAM

42 類比通訊線

五、發明說明（ 8 ）

44 外部類比輸入裝置

52 媒體驅動器

54 監視器

56 滑鼠裝置

64 記憶體

66 CPU

68 可移除式磁碟控制器

72 軟碟控制器

74 軟碟機

76 硬碟機

78 磁帶機

80 CD-ROM 驅動器

101 AIC 晶片

102 SCSI

103 DMA

104 磁碟格式化器

105 PHAEDRUS

106 微控制器

107 RAM

108 應用特定積體電路(ASIC)

本發明係提供用於從一遠端伺服器經由一網路基礎結構而將敏感性或受保護之電子資料傳送至一用戶電腦或是單機裝置的一種安全的方法，並且一旦資料係遞送至用戶電腦或是單機裝置，則防止該資料之未經授權的分配以及

五、發明說明（ 9 ）

拷貝。如在此所使用者，「資料」一詞係包括可儲存在一儲存媒體上之所有資訊(包括之而不限於此)，可執行的檔案，鏈結的程序庫檔案，資料檔案，資料庫檔案，音頻檔案，以及視頻檔案。

參照第一圖至第四圖，係顯示有一個示範性而非限制性的環境 10 以及裝置，其中係可實施本發明。如第一圖所示，該環境 10 係包括一寬域網路(WAN)基礎結構 12。該 WAN 基礎結構 12 可包括一傳輸控制協定/網際網路協定(TCP/IP)網路，例如網際網路。經由通訊線 24 而附接至該 WAN 基礎結構 12 的可以是一或多個區域網路(LAN)14，伺服器 16，網際網路服務提供器 18，以及可與該 WAN 基礎結構 12 之協定相容的單機裝置 22。如所示者，該 LAN 14 以及網際網路服務提供器(ISP)18 可附接至用戶個人電腦/工作站 20 及/或單機裝置 22，其可經由該 LAN 14 或是 ISP 18 而接達至該網路基礎結構 12，其並且至少能夠接達以及讀取在可移除之媒體 28 上的資料。亦顯示的是一資料解密/解壓縮裝置 30，其係可附接至一個人電腦/工作站 20 。

該 LAN 14 可包括一乙太網路或是表號環式網路，並且具有一伺服器 16 以及網間連接器(未圖式)，該網間連接器係提供經由一或多個通訊鏈路 24 而至該網路基礎結構 12 的連接。至遠端系統的該通訊鏈路 24 可爲無線鏈路，衛星鏈路，或是專用線路。

舉例而言，該伺服器 16 可包括具有一或多個處理器(

五、發明說明（10）

例如 Intel Pentium II 處理器，數位設備公司 Alpha RISC 處理器，或是 Sun SPARC 處理器)之 UNIX 基礎或是 Windows NT 伺服器基礎之電腦平台，長期儲存器(例如 RAID 磁碟陣列)，隨機存取記憶體(RAM)，通訊週邊設備(例如網路介面卡，數據機，及/或中端轉接器)，以及應用程式(例如資料庫軟體應用，全球寬域網路（World Wide Web）出版/主軟體，以及庫存管理軟體)，其可用於分配資訊至用戶個人電腦/工作站 20，單機裝置 22，以及其他伺服器 16。舉例而言，該等伺服器 16 可構成爲全球寬域網路（WWW）伺服器，檔案傳輸協定(FTP)伺服器，電子郵件(E-mail)伺服器等等。該 ISP 18 典型上爲一機構或服務，其係提供經由一伺服器(未圖示)接達至網際網路(網路基礎結構 12)之通路，該伺服器係藉由通訊鏈路 24 連接至網際網路。在第一圖之示範實施例中，該用戶個人電腦 20 或是單機裝置 22 可使用一撥號(dial-up)連接 26(經由公共交換電話網路)以連接至該 ISP 18。

該用戶個人電腦 20 可包括視窗 95，視窗 98 或是視窗 NT 工作站基礎個人電腦，其具有 Intel Pentium 處理器或更高階者，長期儲存器(例如一 IDE 或是 SCSI 硬碟)，一可移除式媒體驅動器(例如 CD-R，DVD-RAM，或其他可移除式軟碟或是硬碟機)，隨機存取記憶體(RAM)，通訊週邊設備(例如網路介面卡，數據機，及/或中端轉接器)，以及合適的應用程式(例如撥號連網軟體以及一全球寬域網路瀏覽器)。如果是構成爲一工作站，則舉例而言，工作站 20 可

五、發明說明（ 11 ）

包括 UNIX 基礎之 IBM RS/6000 或是 SUN SPARCS 工作站等工作站。甚且，該用戶個人電腦/工作站 20 可包括所謂的「網路計算」裝置。

一示範的個人電腦/工作站 20 之方塊圖係顯示於第二圖。如所示者，個人電腦/工作站 20 係分割成內部以及外部組件。該內部組件係包括一基本輸入/輸出系統(BIOS)以及控制該個人電腦/工作站 20 之全部功能的一處理器(CPU)66。記憶體 64，一硬碟機 76，一軟碟機 74，一磁帶機 78，一 CD-ROM 驅動器 80，一數據機/終端轉接器/網路介面卡 82，以及一可移除式媒體驅動器 52a 亦係連接至該 CPU 66。該可移除式媒體驅動器 52a 或 52b 係操作以讀取及/或寫入包含在一可移除是儲存卡匣 28 中之儲存媒體。第二圖之示範的個人電腦/工作站 20 係構成有二個可移除式媒體驅動器 52a 或 52b 以強調一可移除式媒體驅動器係可以內部或是外部形式實施。

該數據機/終端轉接器/網路介面卡 82 可包括實行通訊相關功能之個別卡，如在此項技藝中已知者。該數據機/終端轉接器/網路介面卡 82 係包括在個人電腦/工作站 20 之中以提供至外部網路的通訊，該個人電腦/工作站 20 即係連接至該外部網路。明確而言，該數據機/終端轉接器/網路介面卡 82 可用於接達 LAN 14，ISP 18 以及網路基礎結構 12。

在內部與外部之間的通訊可經由提供於該個人電腦/工作站 20 中的控制器而達成。一串列/並列/USB 部控制器(

五、發明說明（12）

其可包括分開的控制器)58，一監視器控制器(視訊卡)60，以及一鍵盤以及滑鼠控制器 62，其各在 CPU 66 與一外部可移除式媒體驅動器 52b(或是印表機)，監視器 54，以及鍵盤以及滑鼠裝置 56 之間分別提供一介面。一硬碟以及軟碟控制器 72 係作用爲分別在該 CPU 66 與該硬碟 76 以及該 CD-ROM 驅動器 80，以及軟碟 74 和磁帶機 78 之間的一個介面。熟知此項技藝者將可知曉，磁碟控制器 72 可包括分開的軟碟以及硬碟控制器(例如 IDE 或是 SCSI 控制器)。

一可移除式媒體控制器 68 係作用爲在該可移除式媒體驅動器 52a 與該 CPU 66 之間的一個介面。舉例而言，該可移除式磁碟控制器 68 可包括一小型電腦系統介面(SCSI)或是積體驅動電子(IDE)介面控制器。一硬碟以及軟碟控制器 72 係作用爲分別在該 CPU 66 與該硬碟 76 以及該 CD-ROM 驅動器 80，以及該軟碟 74 和磁帶機 78 的介面。或者，該可移除式媒體驅動器 52a 可利用該磁碟控制器 72 作爲對該 CPU 66 的一個介面。

現在參照第三圖，顯示有一示範媒體驅動器 52 的方塊圖，該媒體驅動器 52 係具有對該個人電腦/工作站 20 的一 SCSI 介面(經由控制器 68)。該媒體控制器 52 較佳係包括一 ZIP® 驅動器，其係由 Iomega 公司，Roy， Utah 所製造；然而亦可使用其他的媒體驅動器作爲媒體驅動器 52。該媒體驅動器 52 係包括提供以用於該媒體的讀取/寫入通道(圖式之右下側)與該個人電腦/工作站 20(圖式之左上側)

五、發明說明（13）

之間通訊的組件。該媒體驅動器 52 係包括一 AIC 晶片 101，其係實行 SCSI 102，直接記憶體存取(DMA)103，以及磁碟格式化器 104 功能。該介面一包括一 PHAEDRUS 105，其係包括一 8032 微控制器 106，一 1k 位元組之 RAM 107 以及一應用特定積體電路(ASIC)108。該 ASIC 108 可實行各種功能，像是伺服排序，資料分配，EOC，ENDEC，類比至數位，以及數位至類比轉換。在該媒體驅動器 52 與該個人電腦/工作站 20 之間的通訊經由在該媒體驅動器 52 之輸入/輸出通道與該個人電腦/工作站 20 之該媒體控制器 68(例如 SCSI 控制器)之間的資料轉移來達成。

再度參照第一圖，如在此所使用者，該單機裝置 22 可包含任何可與該網路基礎結構 12 交互作用的裝置，不同於「傳統」的計算裝置(亦即 PCS，工作站，網路電腦，或是終端機)。舉例而言，該單機裝置 22 可包括像是 WebTV®(其係由 WebTV Networks, Palo Alto, California, 所供銷)，一音樂或是影片播放器等之類的裝置。應注意的是該單機裝置並不需要設置對該網路基礎結構，LAN，或是 ISP 的通訊連接。

一個示範的單機裝置 22 之方塊圖係顯示於第四圖。該示範的單機裝置 22 係包括一可移除式媒體驅動器 52a，一可移除式媒體控制器 68，一 CPU 66，一 ASIC/控制器 36，一數位至類比轉換器 38，ROM 37，以及 RAM 39。如同熟知此項技藝者所可知曉者，第四圖之單機裝置 22 可藉由從該媒體 28 讀取受保護之資料而操作爲該受保護之資料的

五、發明說明（14）

一「播放器」或是「觀賞器」。該可移除式媒體驅動器 52a，該可移除式媒體控制器 68，以及該 CPU 66 各操作如同在第一圖至第三圖之個人電腦/工作站 20 中所敘述者。ROM 37 係包含用以控制該單機裝置 22 之操作以及功能的指令。該 ASIC/控制器 36 可被使用於將該受保護之資料解密並且輸出數位音頻及/或視頻信號(例如脈衝編碼調變(PCM))至該數位置類比轉換器 38 以用於轉換成類比音頻或是視頻信號。

再度參照第一圖，顯示有根據本發明之一解密/解壓縮裝置 30，其係連接至個人電腦 20 以實行受保護之電子資料的讀取/播放/執行。該解密/解壓縮裝置 30 與該單機裝置 22 的不同之處在於該解密/解壓縮裝置 30 並未設置一裝置(例如可移除式媒體驅動器 52)來讀取該媒體 28，而是接收由該個人電腦/工作站 20 通訊並且讀取的資料。

應注意的是在第一圖至第四圖中所示之示範性環境以及裝置並不限制於所示之環境，而其他的網路基礎結構，通訊連接，以及裝置係傾向於在本發明之範疇以及精神中。

現在參照第五圖，顯示有根據本發明之電子分配模型而實行之程序。如對於熟知此項技藝者將明瞭者，本發明之特徵以及特點係可藉由硬體，軟體及/或韌體之任合適當的組合而實施。根據本發明，該網路伺服器或諸伺服器 16 可儲存資料，像是應用軟體，資料庫表格，音樂，影片等等，以用於分配給用戶 20 及/或單機裝置 22。雖然本發明

五、發明說明（15）

可應用於所有類型的資料傳輸，但是由其可應用在網際網路上交易，並且明確而言，針對軟體，音樂以及影片資料之電子分配。

本發明係利用一公共鑰匙，或是非對稱的加密方式來將從該伺服器 16 下載至該用戶裝置 20(或 22)之資料加密。根據非對稱之加密，係在加密/解密程序中使用一對鑰匙：一公共鑰匙，其係給予預加密資料之任何人，以及一專用鑰匙，只有欲解密該資料的人知道它。對照於對稱式加密，用於解密的鑰匙永遠與用於加密的鑰匙不同。公共鑰匙加密之更詳細的說明係可見於應用密碼使用解譯法：協定，算則，以及於 C 之來源碼，由 Bruce Schneier 所著，第二版(1995 年十二月)，John Wiley & Sons 出版，係在此整體納入作爲參考。

非對稱式加密的一個優點是在於加密方法的不可破解性係依據該等鑰匙之長度(亦即位元的數目)。由於現在的電腦使得可以採用非常長的鑰匙，可以採用相當長的鑰匙以致要花費數千年或更久來將之破解。非對稱鑰匙的一個缺點係在於對稱式算則(集中加密/解密鑰匙爲相同)要比公共鑰匙系統快 1000 倍，因此在大量資料之即時上使用非對稱系統是不實際的。如同以下將說明者，本發明係利用兩種加密方法之力量來防止一旦資料傳送至一目的媒體之後，經下載之資料(受保護之內容)被非授權拷貝。

根據本發明，對於欲保護之經加密的電子資料的資料鑰匙係在下載程序期間利用公共鑰匙加密而加密，並且該

五、發明說明（16）

資料係利用該媒體 28 之唯一的識別子(例如序列號碼)作爲一加密鑰匙而下載以及加密至該媒體 28。在另一個實施例中，該資料係利用一複合鑰匙作爲加密鑰匙而加密至該媒體 28，該複合鑰匙係包括該媒體 28 之唯一的識別子，一販售者識別子以及使用者識別子。爲了確保媒體 28 之各特定塊均具有一唯一的識別子，該唯一的識別子係在製造過程期間永久性地埋入該媒體 28，並且係不可由使用者或是讀/寫該媒體 28 之磁碟機以在之後接達。甚且，該媒體之使用者格式將不會抹除或是更改該埋入的序列號碼。因此，該下載之加密的受保護之電子資料而後係藉由該唯一的識別子而與該媒體 28 相關聯並且不可由任何其他具有不同的唯一的識別子或不具有識別子之媒體接達。此外，如果使用複合鑰匙以將資料寫入該媒體 28，則該受保護之電子資料係不可由任何其他的媒體接達，並且如果該販售者或是使用者識別子不正確則亦不可接達。

參照第五圖，在一使用者於用戶個人電腦 209 單機裝置 220 上經由例如一寬域網路瀏覽器而與一伺服器 16(寬域網路伺服器)接觸並且連接，以及選擇欲下載的受保護之資料之後，程序在步驟 200 開始。當使用者想要利用一家用個人電腦 20 或是單機裝置 22 來購買軟體，音樂或是影片(亦即受保護之電子資料)時，該使用者係在步驟 200 開始電子資料分配程序。受保護之電子資料可從駐在伺服器 16 之一上之例如全球寬域網路(WWW)位置提供以一費用販賣，並且係利用信用卡，簽帳卡，聰明卡(smart card)，

五、發明說明（17）

虛擬現金等等來購買。爲了此項目的，該家庭使用者可經由一網際網路瀏覽器(像是由 Microsoft, Redmond, WA 所供銷的網際網路 Explorer)而連接(步驟 202)至 WWW 位置器，其係藉由進入通用資源位置器(URL)或是「點選(clicking)」包含 WWW 位置之 URL 的超本文連結。該 URL 可包含例如一網際網路協定(IP)位址(例如 147.178.20.151)或是一轄域名稱(例如「sitename.com」)，其係確認該位置的 IP 位址，以便該瀏覽器可建立一 TCP/IP 連接。較佳而言，該寬域網路伺服器 16 係包括一 Iomega 儲存網伺服器 16，其在下文將加以說明。亦較佳的是，至該寬域網路伺服器之連接係一安全的(亦即加密的)連接。在該使用者從該寬域網路伺服器點選所顯示之網頁的下載按鈕之後，此項動作係致使該個人電腦/工作站提出一 HTML 格式至該寬域網路伺服器 16。該寬域網路伺服器 16 而後係執行適合的共用網間連間器介面(CGI)程式。在 Iomega 儲存網伺服器 16 上運作的 CGI 程式係傳送元標記「Content-Type: application/x-itf」，隨後是一合適的 Iomega 事務處理檔(ITF)至該用戶個人電腦/工作站 20。該 ITF 檔對於該 Iomega 儲存網伺服器 16 而言是唯一的，並且係用於提供資訊至一 ITF 用戶程式，其係控制在用戶側之下載程序。該 ITF 檔之格式係顯示於第八圖。隨著該寬域網路瀏覽器接收該元標記，其係啓動該 ITF 用戶程式並且將該 ITF 檔案名稱當成一指令線參數。該 ITF 用戶應用係打開該 ITF 檔並且剖析來自該元標記之元資料。該用戶

五、發明說明（18）

個人電腦/工作站 20 係連接至由 ITFSERVER 標記所提供的伺服器位址以接收該電子資料(見步驟 308)。該伺服器位址可對於各個請求而動態改變以平衡在該伺服器上之負載。舉例而言，該 ITF 檔可包括下列之用於傳輸包含一首歌之單一檔案的資訊：

<ITFVERSION:>0.1
<ITFNEWFILE:>
<ITFID:>2
<ITFSERVER:>147.178.20.151
<ITFFILENAME:>D:\WebSite\htdocs\html\ZipMan\Samples\
SuppReady.mp3
<ITFARTIST:>Genesis
<ITFTITLE:>Supper's Ready
<ITFALBUM:>Foxtrot
<ITFCOST:>$2.50
<ITFDATE:>3/4/98
<ITFSIZE:>4746500

在步驟 202，該用戶系統 20(或 22)係產生二個鑰匙，一個公共鑰匙(K1)，以及一個專用鑰匙(K2)。該等鑰匙係具有預定的尺寸並且可利用 ANSI 標準 X9.17 或利用從在用戶裝置硬體上運轉的即時時鐘(一虛擬隨機數字產生器)所取得的一系列數字而產生。

在步驟 204，該用戶個人系統 20 係連接至在

五、發明說明（19）

ITFSERVER 標記(例如 147.178.20.151)中確認的伺服器 16，並且經由 TCP/IP 插槽傳送一指令封包至該伺服器。該第一指令封包係具有一之致動碼，並且係包含欲傳輸的檔案名稱，所有的客戶資訊，帳單資訊，以及該公共鑰匙(K1)。該第一指令封包可被格式化如以下所列：

```
struct SocketCommend
{
  unsigned long   Code;
  unsigned long size;
  unsigned char Data[400];
};
```

或者，資料欄可包括複數個欄位，其係包含客戶資訊，帳單資訊，以及該共鑰匙(K1)以作爲剖析的欄位。該資料欄可被格式化以具有以下的資料結構：

```
{
   char First[20];
   char Last[20];
   char Address[40];
   char City[20];
   char State[3];
   char Zip[6];
   char CreditCard[17]
   char ExpDate[5];
   char Phone[13];
```

五、發明說明（ ）

```
        char Key[128];
        long int DataID;
    };
```

在步驟 206，該伺服器 16 利用用戶之公共鑰匙(K1)以加密拷貝保護資料鑰匙(K3)。該拷貝保護資料鑰匙係用於將儲存在該伺服器 16 上之資料加密/解密的鑰匙。在步驟 208，該伺服器響應於具有相同致動碼之資料封包並且通知用戶 20 已經開啓檔案以及檔案大小。此外，該伺服器 16 係將經加密的拷貝保護資料鑰匙(K3)傳送至用戶 20。在步驟 210，該用戶裝置 20 係利用用戶之專用鑰匙(K2)將該經加密的拷貝保護資料鑰匙(K3)解密。而後該拷貝保護資料鑰匙(K3)可儲存於 RAM 64 以便後續使用以當由用戶裝置 20 接收該拷貝保護資料時將之解密。

在步驟 211，該用戶裝置 20(或 22)係傳送具有二之致動碼的指令封包，其係通知伺服器傳送下一筆 4000 位元組的資料。應注意的是此致動碼係重複執行直到整個檔案已從伺服器 16 傳送至用戶個人電腦 20 或是單機裝置 22(經由步驟 211 至 218 之程序，如以下所述者)。在步驟 212，該伺服器 16 係經由例如 TCP/UP 插槽而將預加密之拷貝保護資料傳送至該用戶裝置 20。從該伺服器 16 傳送至該用戶個人電腦 20 之資料較佳係唯一預定的資料結構，例如以下所列：

五、發明說明（ 7 ）

```
struct SocketData
{
  unsigned int   Code;
  unsigned long size;
  unsigned char Data[4000];
};
```

在步驟 214，該用戶利用該拷貝保護資料鑰匙(K3)來解密該拷貝保護資料。或者，在步驟 212 以及 214，該系統可藉由將預加密之拷貝保護資料利用公共鑰匙第二次加密以便傳送至該用戶裝置 20 而提供雙重加密，並且利用專用鑰匙(K2)以及該拷貝保護鑰匙(K3)加以解密。當步驟 214 完成之時，該資料係在解密狀態並且準備寫入該媒體，以致其根據本發明而與該媒體 28 永久相關聯。

該資料與該媒體 28 之相關聯係在步驟 216 開始，其中該 ITF 用戶程式取得該媒體 28 之唯一的識別子(第一實施例)或是複合鑰匙(第二實施例)而加密，其係用於使該資料與該媒體 28 相關聯。現在參照第六圖，在步驟 300，該 UTF 用戶程式係決定是否是第一次將該部分的受保護之資料寫入該媒體 28。如果是如此，該用戶個人電腦 20 係查詢該媒體之特定的一塊，而所下載的內容係將儲存至該媒體之特定的一塊以用於該媒體之唯一的序列號碼。作爲一個非限制性的例子，該媒體 28 可包括由 Iomega 公司，Roy, Utah 所製造的一 ZIP®磁碟。每個 Iomega ZIP®磁碟係

五、發明說明（ ）

包含一個唯一的序列號碼，該唯一的序列號碼係在格式化程序期間寫入一預定的磁軌，該唯一的序列號碼係可被使用作爲一個唯一的識別子。該序列號碼較佳係藉由一僞隨機號碼產生器所產生，但並不限制於此。甚且，雖然該媒體 28 已經以一 ZIP®磁碟加以說明，但是其並不限制於 ZIP®磁碟，使用其他具有一個唯一的識別子之可移除式或永久式媒體形式亦係在本發明之範疇以及精神內，像是 CD-R，DVD-RAM，以及其他可移除式軟碟以及硬碟。

該用戶個人電腦 20 可利用一應用程式介面(API)來查詢該媒體，該應用程式介面(API)係例如像是 Iomega Ready API，或是其他適合的方法。當被請求時，該 Iomega Ready API 係藉由 SCSI 0x06 Non-Sense 指令致使該媒體驅動器從該預定之磁軌讀取該唯一的序列號碼。明確而言，藉由請求該 Non-Sense 指令之磁碟狀態頁(Disk Status Page) (頁 0x02)，該媒體序列號碼可返回之資料結構的偏移位元組 20-59 而加以決定。用於連同 Iomega ZIP®驅動器以及磁碟來實行步驟 302 之示範來源碼係如下所列：

```
void CclientApp::GetZip Drive()
{
        int j,k;
        m_DriveNum=0;
        for(j=0;j<26;j++)
                //scan the drives and find the IOMEGA drives
        {
                if(IsIomegaDrive(j))
                {
                        k=GetGeneralDevType(j);
                        if(k==DRIVE_IS_ZIP)
```

五、發明說明（ ）

```
                    {
                        m_DriveNum=j;
                        j=26;
                    }
                }
            }
        }

void CclientApp::GetSerialNumber()
{
    unsigned char szBuffer[1024];
    memset(szBuffer,0,sizeof(szBuffer));
    memset(&m_SerialNumber,0,40);
    GetInfoNonSense(m_DriveNum,0x02,szBuffer);
    Memcpy(&m_SerialNumber,&szBuffer[22],39);
}
```

應可知曉該唯一的識別子並不限於在該媒體 28 上所儲存的資訊(例如像是序列號碼)，而其他類型的資訊亦可用作爲唯一的識別子，只要該資訊係永久性地儲存在該媒體 28 上即可。此外，該唯一的序列號碼應包含足夠數目之位元(長度)以確保沒有兩塊媒體會具有相同的識別子。舉例而言，每個 Iomega ZIP®磁碟係包含一個唯一的 39 位元組(312 位元)之序列號碼，而亦可使用其他位元長度。在取得唯一的識別子之後，其係儲存於 RAM 64 以便後續使用。如果在第一實施例之下操作(亦即僅根據唯一的識別子將資料寫入該媒體 28)，則該程序在步驟 312 返回至步驟 217(第五圖)。

然而，根據第二實施例，係藉由在該加密/解密鑰匙中不僅包括該唯一的識別子並亦包括販售者識別子以及使用

五、發明說明（24）

者識別子而提供額外的安全性。此一加密/解密鑰匙在此係稱作爲一複合鑰匙。明確而言，藉由利用具有販售者資訊以及使用者資訊的複合鑰匙，可在受保護之資料的分配中建立額外的安全防護。該販售者資訊可爲由該受保護之內容的販售者或是一企業集團所製造的一識別子。此一識別子的目的係使得該販售者或是企業集團可加上額外的安全層，以防止由個人或軟體程式對於該受保護之資料所行之未由該販售者或企業團體所許可之未經授權的解密。舉例而言，如同以下加討論者，該販售者資訊可由應用軟體下載，執行或播放受保護之內容取出，因此進一步限制該內容對於具有經許可之應用軟體拷貝之裝置的使用。或者，該販售者資訊可從位於一區域網路(LAN)，寬域網路(WAN)，或是網際網路等等之一伺服器取出。

該使用者資訊係一種對於一個別的使用者或一群使用者爲特定的資訊。此識別子可由使用者產生，或依照使用者的習慣藉由應用軟體產生。該使用者識別子係提供使用者對於該受保護之內容之接達的控制。此種使用者控制在合作環境中可能是合乎需求的，其係僅使得經授權的使用者(例如公司職員，特定部門以及特定個人)可接達該受保護之內容。在家庭中，使用者控制係提供父母一種機制以防止兒童接觸不適當的內容(例如 R 級電影)。

根據第二實施例，在步驟 304，係取得該販售者資訊。此種資訊可藉由以知的手段而埋藏在 ITF 用戶程式中，該程式係在用戶側控制下載程序。如此，每個販售者係具

五、發明說明（ 17 ）

有一個唯一的 ITF 用戶程式以實行下載程序。或者，可在用戶側執行一一般性的 ITF 用戶程式，以及販售者資訊係從在用戶個人電腦 20，單機裝置 22 上之檔案，或是從在該伺服器 16 上的資料庫取得，其係使該受保護之內容與該販售者資訊經由以知的程序而相關聯。

在步驟 306，係取得該使用者資訊。此較佳係藉由提示使用者以資訊而實行。該使用者而後係輸入該資訊，該資訊係暫時儲存於 RAM 64 中或是該硬碟 76 上。或者，可訴諸一分離的軟體應用以提供使用者資訊(例如從一網路黃頁檔案取出使用者之密碼的密碼應用)。

在步驟 308，係建立該複合加密/解密鑰匙。該程序可藉由人和手段來組合三個鑰匙成分(例如該媒體 28 之該唯一的識別子，該販售者資訊，以及該使用者資訊) 而實行，該等手段係包括數學運算(mod，相加，相除，相減，XOR 等等)連鎖，插入，或是任何其他方法。較佳而言，係實行該販售者資訊以及使用者資訊之位元組階層插入。此產生具有以下結構的串列：V0U0V1U1V2U2V3U3V4U4V5U5V6U6V7U7，其中 Vx 係販售者資訊位元組 x，而 Ux 係使用者資訊位元組 x。所產生的串列而後係藉由 XOR(互斥 OR)運算而與該唯一的序列號碼組合以構成複合鑰匙。因此，該複合鑰匙較佳係產生如下：

CK=S XOR (V 插入之 U)

其中，

五、發明說明（26）

CK=複合鑰匙

S=序列號碼

V=販售者資訊

U=使用者資訊

而後該程序係進行至步驟 312，集中其係返回步驟 217(第五圖)。

如果在步驟 300 其係由該 ITF 用戶應用判定該下載的資料已經寫至該媒體，該唯一的識別子或是複合鑰匙係已經在步驟 302(第一實施例)或是 308(第二實施例)中取得，並且儲存 RAM 64。如此，在步驟 310，該 ITF 用戶應用係從 RAM 64 回該唯一的識別子或是複合鑰匙並且在步驟 312 返回步驟 217(第五圖)。

應注意的是已經說明該唯一的識別子以及複合鑰匙係被取得並且儲存於該 RAM 中。此係有利地使下載程序加速。然而，爲了確保該媒體 28 不會在下載期間被移除，該唯一的識別子或是複合鑰匙可在每次寫入(藉由重執行步驟 302 以及 304 至 308)該媒體 28 取得。應注意的是此第二種方法可能比上述者較慢，其係肇因於所增加的磁片接達活動。

再度參照第五圖，在步驟 217，該用戶裝置 20 係利用該唯一的串列號碼(第一實施例)或是複合鑰匙(第二實施例)作爲一加密鑰匙而將下載之內容加密。雖然在步驟 217 可使用任何的加密算則，但資料加密較佳係利用廣爲人知的 Blowfish 加密算則來實行。該 Blowfish 加密算則的優點在

五、發明說明（ 27）

於快速，尤其當實施於具有大的資料高速緩衝記憶體之 32 位元的微處理器上時，例如像是 Intel Pentium IBM/Motorola PowerPC。簡言之，Blowfish 是一種可變長度之 64 位元方塊密碼，其係可實施於硬體或是軟體。其算則係由二個部分組成：鑰匙擴充部分以及資料加密部分。該鑰匙擴充部分係將至多 448 位元之鑰匙轉換成總數爲 4168 位元之數個子鑰匙陣列。該資料加密係經由一 16 循環(round)Feistel 網路而發生，其中每一循環係由一鑰匙依存排列以及一鑰匙和資料依存置換所組成。所有的運算係在 32 位元的字元上作互斥 OR(XOR)以及相加。唯一額外的運算係每循環四次索引陣列資料查表以產生經加密的資料。

在步驟 218，該用戶裝置係將經加密之拷貝保護資料寫入媒體 28。該資料可以標準檔案系統結構或是直接軌道或扇段寫入而寫入該媒體 28。資料所寫入該媒體 28 之格式並不受限於所數之格式，其他格式亦可加以使用。

步驟 211 至 218 的程序係一再重複直到所有的資料以從該伺服器 16 下載至該用戶個人電腦 20 爲止。於其時該用戶個人電腦 20 會傳送三之致動碼以通知該伺服器 16 該事務處理已經完成，並且將該插槽斷接(步驟 312)。應注意的是，上述的來源碼以及資料結構係僅爲說明之目的而包括於此，完全沒有限制本發明之範疇的意味。

如上所述，該資料係利用至少該唯一的序列號碼作爲解密鑰匙而以加密格式儲存於該媒體 28。該加密/解密鑰匙

五、發明說明（ 28）

係可爲一複合鑰匙，該複合鑰匙係包括該媒體的唯一的序列號碼，販售者資訊以及使用者資訊。因此，如果該資料被拷貝至任何其他的媒體，則解密程序將會失敗而使得其內容無法使用。所以，利用本發明之裝置以及方法將可防止所下載的資料被未經授權的拷貝。甚且，雖然以上所述之程序係針對一用戶個人電腦，但該程序亦可應用於能夠經由網路基本結構通訊，並且對儲存受保護之電子資料的媒體可讀取以及寫入的單機裝置。舉例而言，可在零售管道設置一亭台(kiosk)，一購買者可將一塊媒體 28 插入該亭台並且在家用或是辦公室個人電腦上下載欲使用的資料。

根據本發明，該伺服器 16 可以加密或未加密格式儲存欲下載之數位內容。如果該欲下載之數位內容並未以加密格式儲存，則其較佳係再下載之時利用該唯一的序列號碼或是複合鑰匙作爲加密鑰匙而加密之。如果該欲下載之數位內容係再下載之前以加密格式儲存在該伺服器 16(預加密)，則該伺服器僅需將該資料鑰匙加密至該內容(亦即軟體應用，音樂或是影片)。預加密可能是較佳的，其係在每件事務有大量資料需要加密的環境中提供更好的性能。如果需要將欲電子分配的整個內容加的話，則此種電子分配系統可能會負擔很重。

一旦經下載的內容已經寫入該媒體 28，其多半會由使用者播放/執行/運作多次。示範性的播放器以及執行或使用所下載之資料的裝置可見於在 1998 年四月 17 日提出申請，標題爲「使用複合鑰匙將保護之電子資料鎖入特別媒

五、發明說明（ 29 ）

體以防止非授權拷貝之系統」之美國專利申請案序號第09/061,493，以及在 1998 年十一月 13 日提出申請 之代理人登錄號 IOM-2793。

應注意的是前述的範例僅提供作爲闡釋之目的而不構成限制本發明。雖然本發明已經參照較佳實施例加以說明，應理解在此所使用之文句係爲說明及闡式之文句而非限制性的文句。甚且，雖然本發明已經參照特定手段，材料以及實施例加以說明，本發明並不傾向受限於在此所揭示之特定者；而是本發明擴展至所有功能性的等效結構，方法以及用途，此等係在所附申請專利範圍之範疇內。得利於本說明書之教示之熟知此項技藝者可實行多種修正以及改變而不悖離本發明於其各方面的範疇以及精神。

舉例說明，本發明可利用具有一唯一的識別子的固定媒體以接收受保護之電子資料。再者，可移除式的媒體並不需要是一可移除式的媒體卡匣，而可包括一可移除式的驅動器，像是經由例如驅動器盤，裝置盤，以及 PCMCIA 插槽而可移除式地連接至個人電腦或是其他裝置者。

## 六、申請專利範圍

1.一種經由網路基礎結構而從伺服器電子分配電子資料至用戶裝置之方法，該方法係利用包括該電子資料下載之一塊之媒體之唯一的識別子的一複合鑰匙以使該電子資料僅與該一塊之媒體相關聯，該方法係包括：

經由該網路基礎結構建立該用戶裝置與該伺服器之間的連接；

產生第一以及第二資料加密鑰匙，該第一以及第二資料加密鑰匙係非對稱式鑰匙；

傳送該第一鑰匙至該伺服器；

根據該第一鑰匙，在該伺服器將該用於該電子資料之受保護之資料鑰匙以及該電子資料至少其中之一加密；

將該電子資料通訊至該用戶裝置；

根據該第二鑰匙，在該用戶裝置將該用於該電子資料之受保護之資料鑰匙以及該電子資料至少其中之一解密；

在該用戶裝置利用該唯一的識別子將該電子資料加密；以及

該電子資料寫入該一塊之媒體，以致該資訊僅可從該一塊之該目的媒體接達以便使用。

2.如申請專利範圍第 1 項所述之方法，進一步包括：

接達該一塊之目的媒體；以及

從該一塊之目的媒體上的一個預定位置讀取該唯一的識別子。

3.如申請專利範圍第 2 項所述之方法，進一步包括：

取得販售者識別子；以及

六、申請專利範圍

取得使用者識別子，

其中在該用戶裝置係利用該唯一的識別子，該販售者識別子以及該使用者識別子加密該電子資料的步驟係進一步包括經由一預定的運算而利用該唯一的識別子，該販售者識別子以及該使用者識別子建立該複合鑰匙；以及利用該複合鑰匙將該電子資料加密。

4.如申請專利範圍第 2 項所述之方法，其中該一塊之目的媒體上的該預定位置係一預定的軌道。

5.如申請專利範圍第 1 項所述之方法，其中將欲傳送至該用戶裝置之該電子資料加密係包括將用於該電子資料之該受保護資料鑰匙以及該電子資料加密。

6.如申請專利範圍第 1 項所述之方法，其中建立該用戶裝置與該伺服器經由網路基礎結構的連接係包括：

從該用戶裝置提供一形式至該伺服器；

在該伺服器執行一程式以處理該形式；以及

傳送一元標記以及事務處理檔至用戶。

7.如申請專利範圍第 6 項所述之方法，其中該元標記以及該事務處理檔係於傳送至該用戶裝置之後，在該用戶裝置啓動一用戶程式。

8.如申請專利範圍第 7 項所述之方法，其中該用戶程式係打開該事務處理檔並且剖析來自在該事務處理檔中之元標記的元資料，以及其中該用戶係連接至藉由在該事務處理檔中之一個預定的元標記而確認的伺服器位址以接收該電子資料。

六、申請專利範圍

9.如申請專利範圍第 8 項所述之方法，其中該伺服器位址係隨著從伺服器要求該電子資料而動態改變。

10.如申請專利範圍第 1 項所述之方法，其中將該電子資料通訊至該用戶裝置係包括將該受保護之資料鑰匙通訊至該用戶裝置。

11.一種用於經由網路基礎結構通訊電子資料的裝置，該裝置係利用非對稱式加密以及該電子資料下載之一塊之媒體之唯一的識別子的一複合鑰匙以使該電子資料僅與該一塊之媒體相關聯，該裝置係包括：

一通訊介面，其係接至該網路基礎結構；

一處理器，其係控制並且執行指令已從該一塊之媒體讀取該電子資料以及該唯一的識別子；以及

一媒體驅動器，響應於該處理器，其係從插入於其中之該一塊之媒體讀取該唯一的識別子；

其中該裝置係經由該網路基礎結構建立與伺服器的連接並且將一第一資料鑰匙通訊至該伺服器，

其中該伺服器根據該第一資料鑰匙將該用於該電子資料之受保護之資料鑰匙以及該電子資料至少其中之一加密並且將該電子資料通訊至該裝置，其中該裝置係根據該第二資料鑰匙而將該用於該電子資料之受保護之資料鑰匙以及該電子資料至少其中之一解密，以及

其中該裝置係利用該唯一的識別子而將該電子資料加密並且將該電子資料寫入該一塊之媒體，以致該電子資料係僅可從該一塊之媒體接達以便使用。

六、申請專利範圍

12.如申請專利範圍第 11 項所述之裝置，其中該裝置係從在該一塊之目的媒體上的一用定位置讀取該唯一的識別子。

13.如申請專利範圍第 12 項所述之裝置，其中該裝置係進一步取得販售者識別子以及使用者識別子，其中將該電子資料加密係利用一複合鑰匙實行，該複合鑰匙係利用該唯一的識別子，該販售者識別子以及該使用者識別子，經由一預定之運算而產生。

14.如申請專利範圍第 11 項所述之裝置，其中該伺服器係在將該電子資料通訊至該裝置之前將用於該電子資料之受保護之資料鑰匙以及該電子資料加密。

15.如申請專利範圍第 11 項所述之裝置，其中該裝置係通訊一形式至該伺服器，其中該伺服器係處理該形式，以及其中裝置係接收一元標記以及事務處理檔。

16.如申請專利範圍第 15 項所述之裝置，其中該元標記以及該事務處理檔係在該裝置啓動一用戶程式。

17.如申請專利範圍第 16 項所述之裝置，其中該用戶程式係打開該事務處理檔並且剖析來自在該事務處理檔中之元標記的元資料，以及其中該裝置係連接至藉由在該事務處理檔中之一個預定的元標記而確認的伺服器位址以接收該電子資料。

18.如申請專利範圍第 17 項所述之裝置，其中該伺服器位址係隨著從伺服器要求該電子資料而動態改變。

19.一種根據公共鑰匙加密用於經由網路基礎結構通訊

六、申請專利範圍

電子資料的裝置，該裝置進一步根據一複合鑰匙以使該電子資料僅與電子資料所下載之該一塊之媒體相關聯，該裝置係包括：

一通訊介面，其係接至該網路基礎結構；

一處理器，其係控制並且執行指令以從該一塊之媒體讀取該電子資料以及該唯一的識別子；以及

一媒體驅動器，響應於該處理器，其係從插入於其中之該一塊之媒體讀取該唯一的識別子；

其中該裝置係經由該網路基礎結構建立與伺服器的連接並且將公共鑰匙通訊至該伺服器，

其中該伺服器根據該公共鑰匙將該用於該電子資料之受保護之資料鑰匙加密並且將該電子資料通訊至該裝置，其中該裝置係根據一專用鑰匙而將該用於該電子資料之受保護之資料鑰匙解密，以及

其中該裝置係利用該複合鑰匙而將該電子資料加密，該複合鑰匙係經由一預定運算，利用該唯一的識別子，販售者識別子以及使用者識別子而產生，並且將該電子資料寫入該一塊之媒體，以致該電子資料係僅可從該一塊之目的媒體接達以便使用。

20.如申請專利範圍第 19 項所述之裝置，其中該販售者識別子以及該使用者識別子係藉由在該裝置上運作之用戶程式取得，並且其中該用戶程式係在依從伺服器接收到一元標記以及事務處理檔即被啓動。

21.如申請專利範圍第 20 項所述之裝置，其中該用戶

六、申請專利範圍

程式係打開該事務處理檔並且剖析來自在該事務處理檔中之元標記的元資料，以及其中該用戶係連接至藉由在該事務處理檔中之一個預定的元標記而確認的動態指派之伺服器位址以接收該電子資料。

22.一種根據公共鑰匙加密用於經由網路基礎結構通訊電子資料的裝置，該裝置進一步根據一複合鑰匙以使該電子資料僅與電子資料所下載之該一塊之媒體相關聯，該裝置係包括：

一通訊介面，其係接至該網路基礎結構；

一處理器，其係控制並且執行指令以從該一塊之媒體讀取該電子資料以及該唯一的識別子；以及

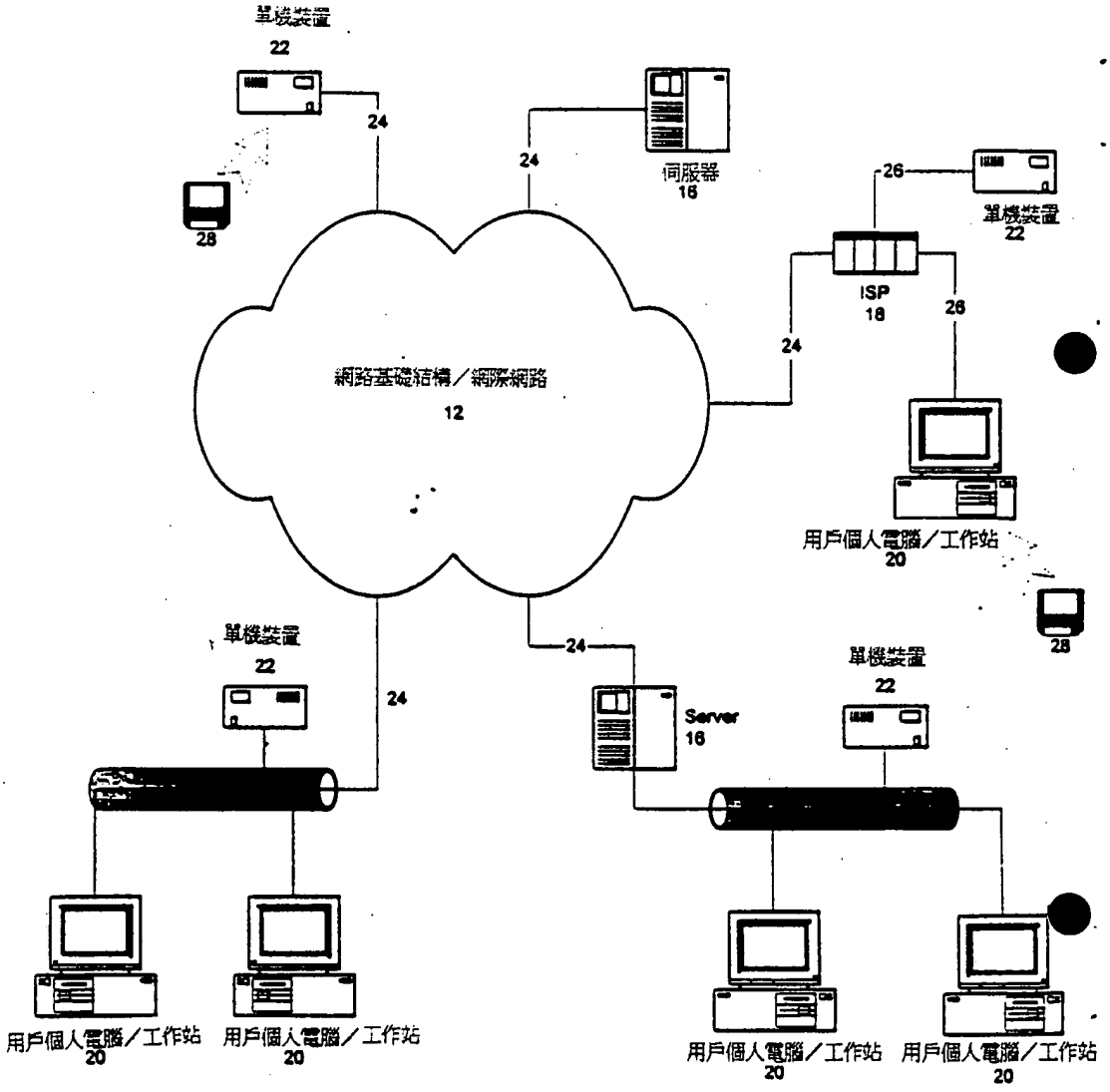
一媒體驅動器，響應於該處理器，其係從插入於其中之該一塊之媒體讀取該唯一的識別子；

其中該裝置係經由該網路基礎結構建立與伺服器的連接並且將公共鑰匙通訊至該伺服器，

其中該伺服器根據該公共鑰匙將該用於該電子資料之受保護之資料鑰匙加密並且將該電子資料通訊至該裝置，其中該裝置係將該受保護之資料鑰匙以及該電子資料寫入該一塊之媒體，以及

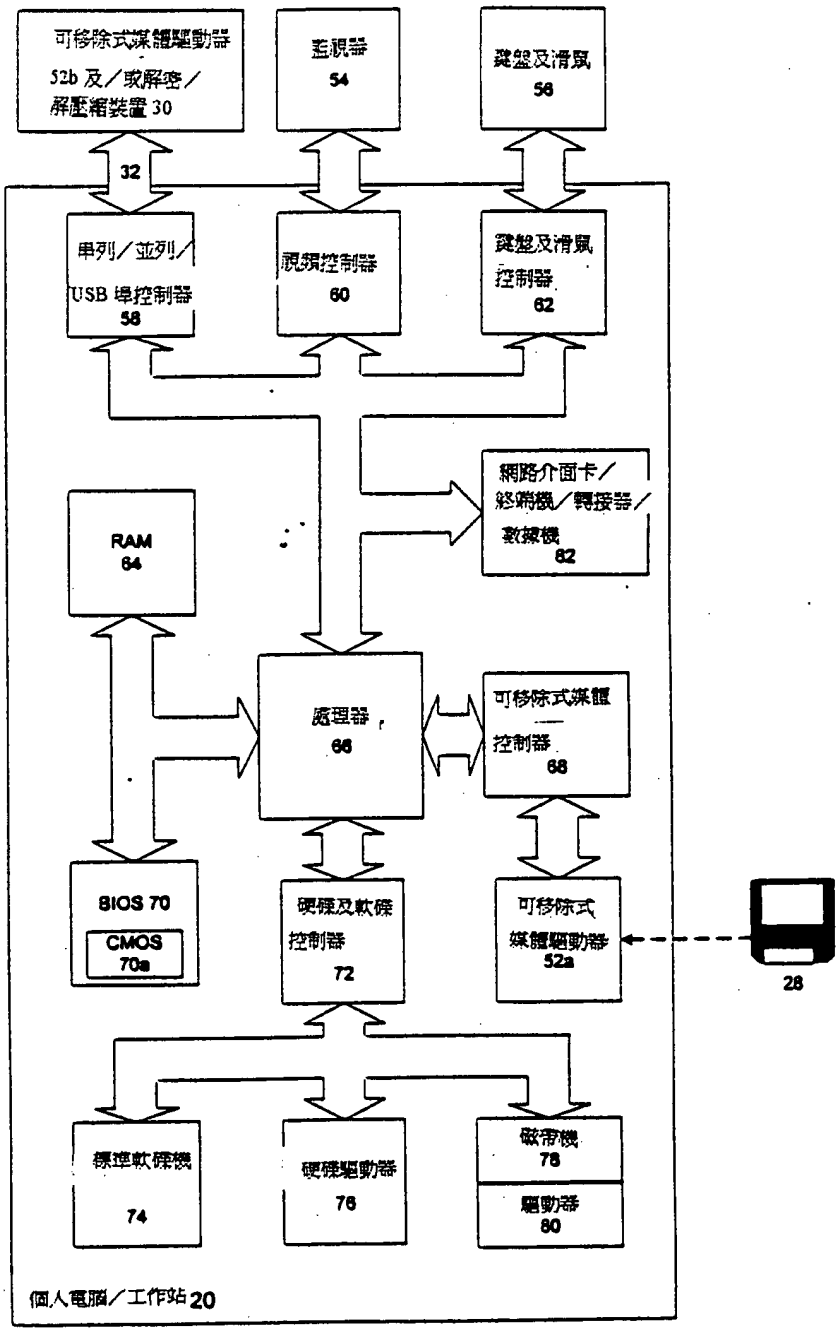
其中該裝置係根據駐留在該裝置一專用鑰匙而將該受保護之資料鑰匙解密並且根據該資料鑰匙而將該電子資料解密，以致該電子資料係僅可從該一塊之目的媒體接達以便使用。

# 第一圖

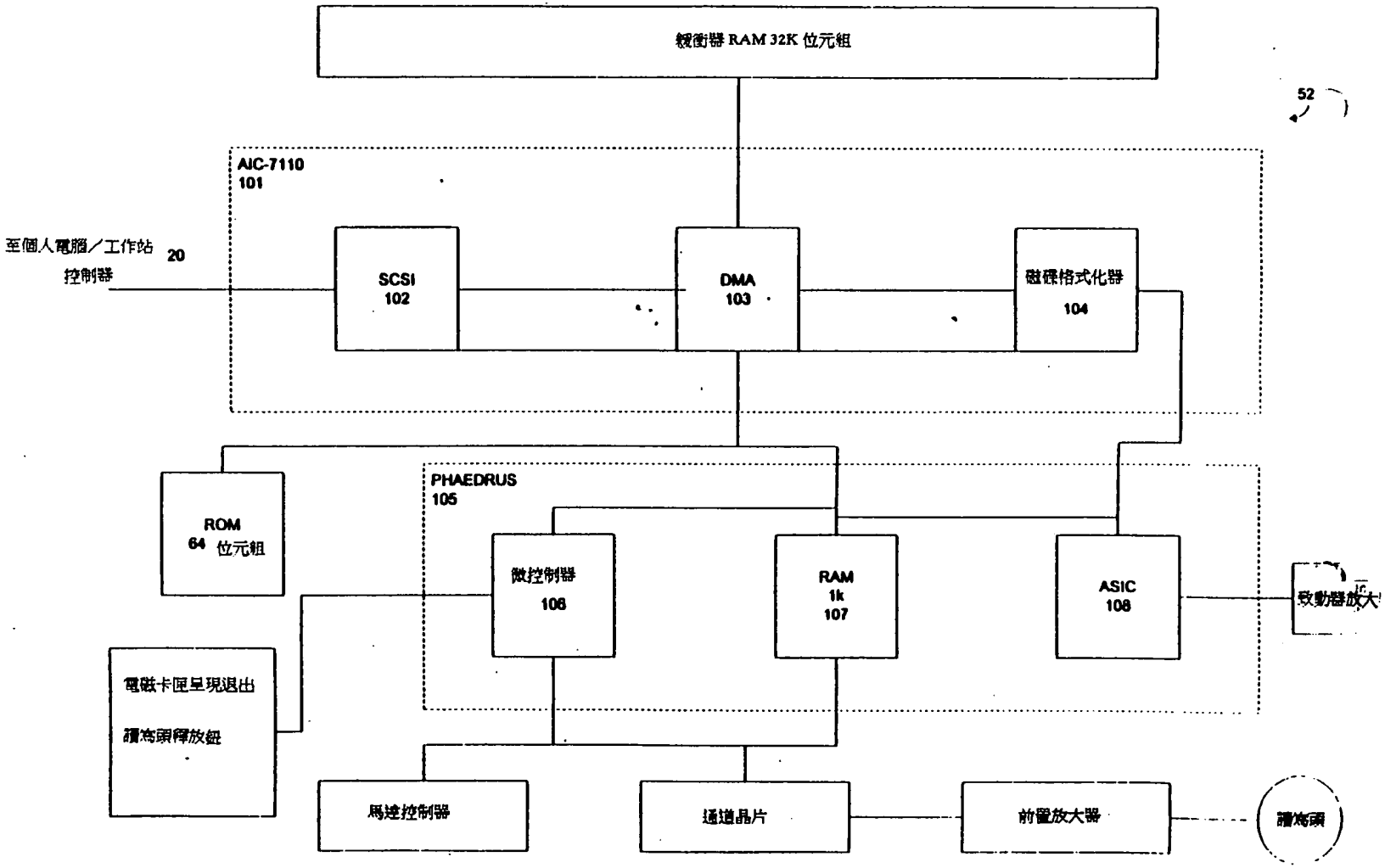

單機裝置
22
24
伺服器
16
26
單機裝置
22
28
ISP
18
26
24
網路基礎結構／網際網路
12
用戶個人電腦／工作站
20
28
單機裝置
22
24
24
Server
16
單機裝置
22
用戶個人電腦／工作站
20
用戶個人電腦／工作站
20
用戶個人電腦／工作站
20
用戶個人電腦／工作站
20

10

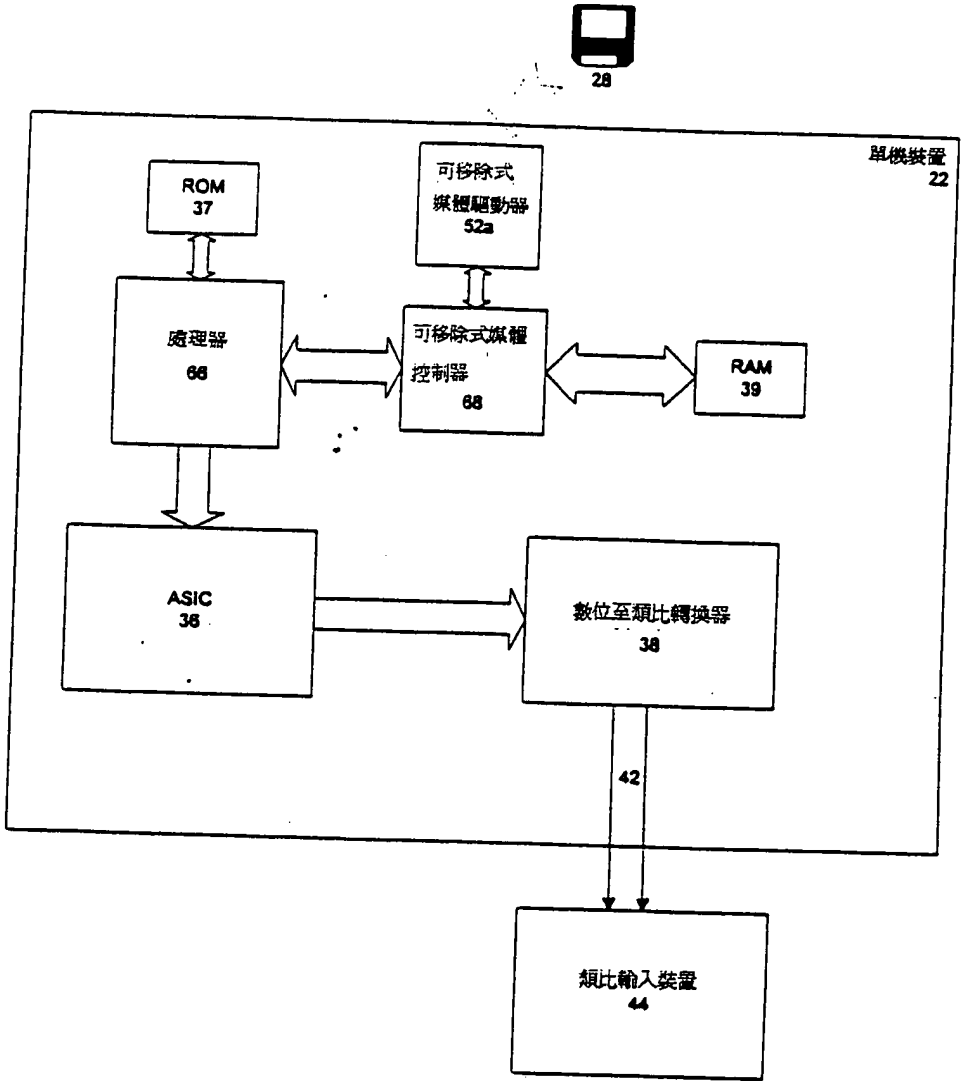
# 第二圖


可移除式媒體驅動器
52b 及／或解密／
解壓縮裝置 30
監視器
54
鍵盤及滑鼠
56
32
串列／並列／
USB 埠控制器
58
視頻控制器
60
鍵盤及滑鼠
控制器
62
網路介面卡／
終端機／轉接器／
數據機
82
RAM
64
處理器
66
可移除式媒體
控制器
68
BIOS 70
CMOS
70a
硬碟及軟碟
控制器
72
可移除式
媒體驅動器
52a
28
標準軟碟機
74
硬碟驅動器
76
磁帶機
78
驅動器
80
個人電腦／工作站 20

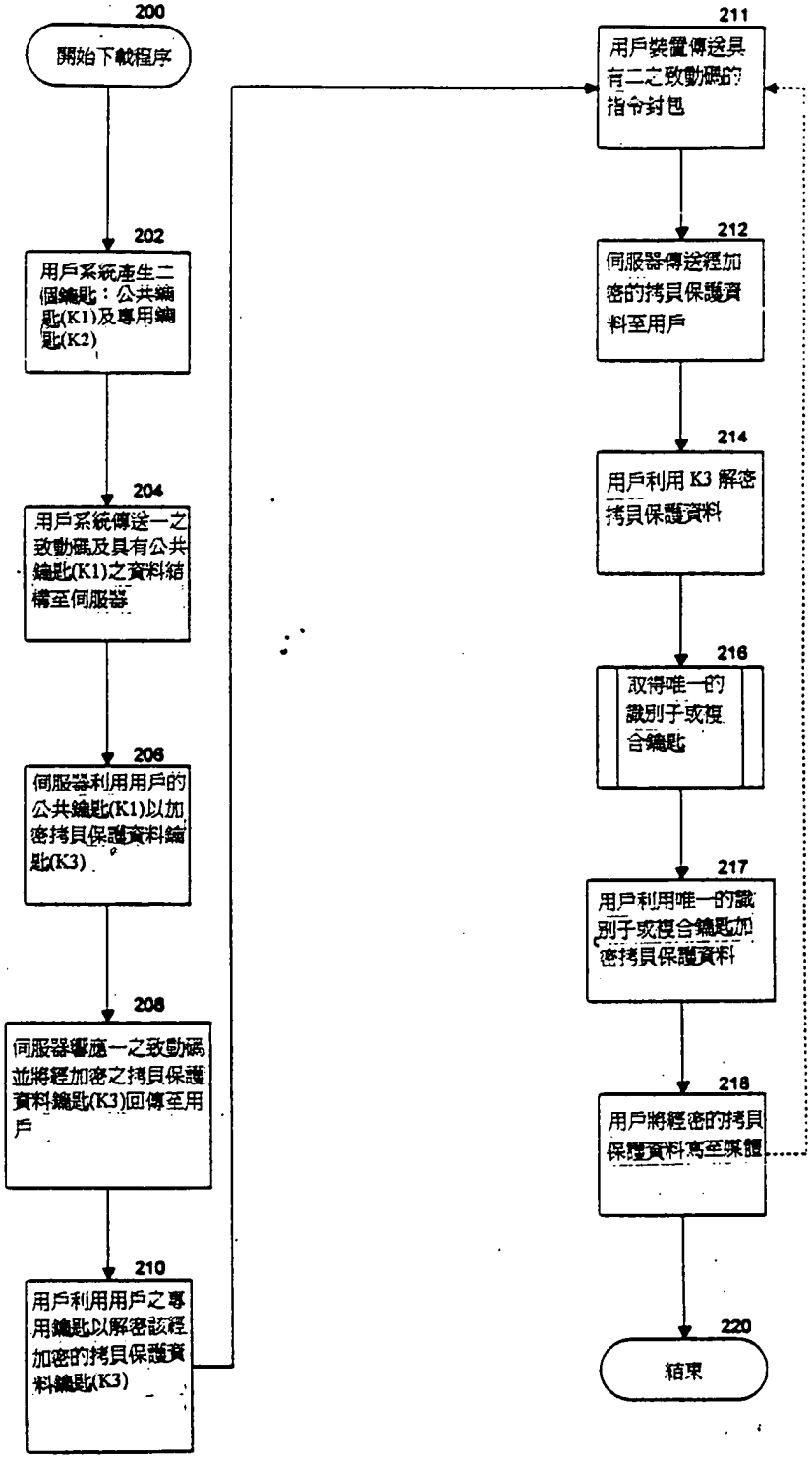
# 第三圖


緩衝器 RAM 32K 位元組
52
AIC-7110
101
至個人電腦／工作站
20
控制器
SCSI
102
DMA
103
磁碟格式化器
104
PHAEDRUS
105
ROM
64 位元組
微控制器
106
RAM
1k
107
ASIC
108
致動器放大
電磁卡匣呈現退出
讀寫頭釋放鈕
馬達控制器
通道晶片
前置放大器
讀寫頭

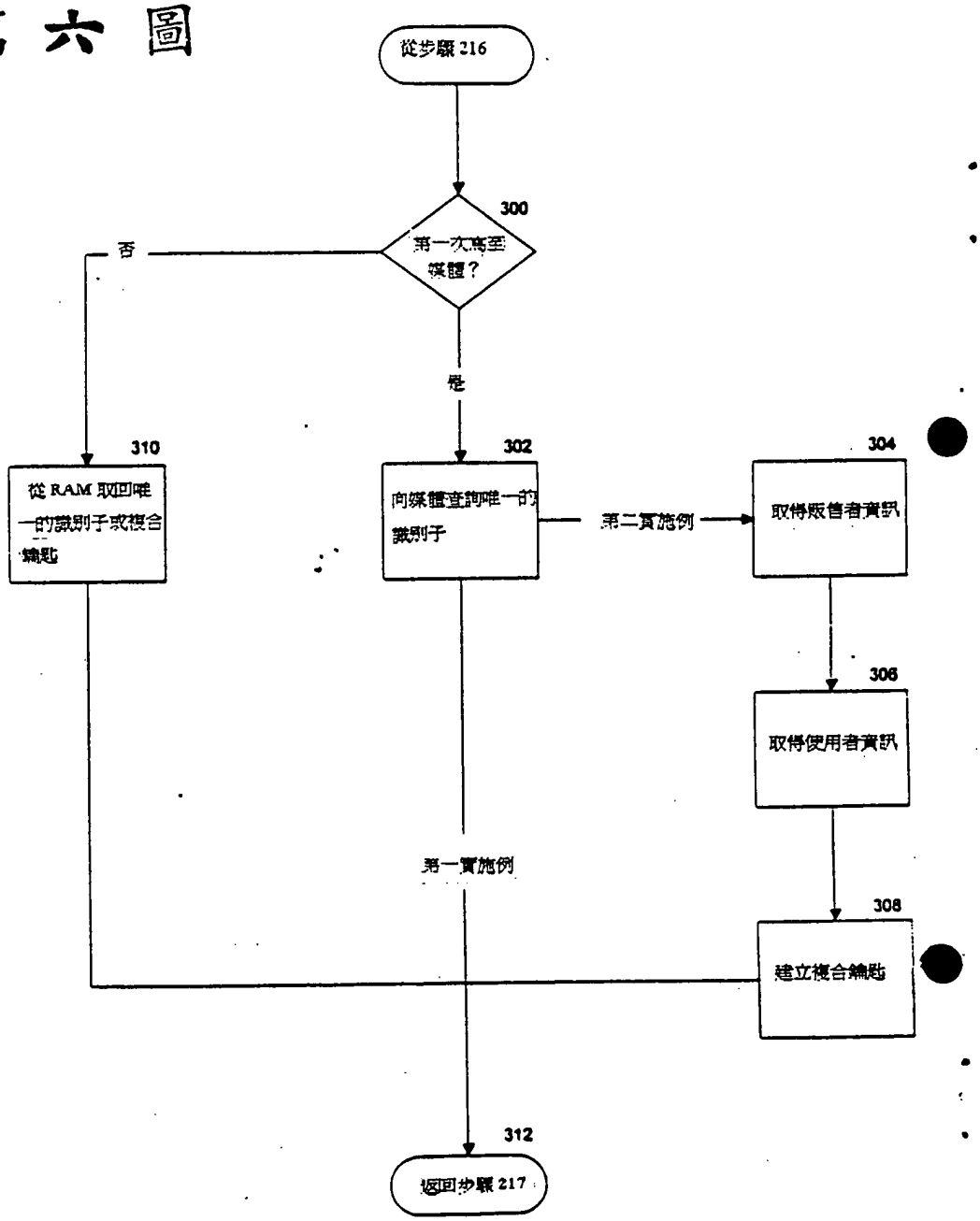
# 第四圖


28
單機裝置
22
ROM
37
可移除式
媒體驅動器
52a
處理器
66
可移除式媒體
控制器
68
RAM
39
ASIC
36
數位至類比轉換器
38
42
類比輸入裝置
44

# 第五圖


200
開始下載程序
202
用戶系統產生二個鑰匙：公共鑰匙(K1)及專用鑰匙(K2)
204
用戶系統傳送一之致動碼及具有公共鑰匙(K1)之資料結構至伺服器
206
伺服器利用用戶的公共鑰匙(K1)以加密拷貝保護資料鑰匙(K3)
208
伺服器響應一之致動碼並將經加密之拷貝保護資料鑰匙(K3)回傳至用戶
210
用戶利用用戶之專用鑰匙以解密該經加密的拷貝保護資料鑰匙(K3)
211
用戶裝置傳送具有二之致動碼的指令封包
212
伺服器傳送經加密的拷貝保護資料至用戶
214
用戶利用 K3 解密拷貝保護資料
216
取得唯一的識別子或複合鑰匙
217
用戶利用唯一的識別子或複合鑰匙加密拷貝保護資料
218
用戶將經密的拷貝保護資料寫至媒體
220
結束

# 第六圖


從步驟 216
300
第一次寫至媒體？
否
是
310
從 RAM 取回唯一的識別子或複合鑰匙
302
向媒體查詢唯一的識別子
第二實施例
304
取得販售者資訊
306
取得使用者資訊
第一實施例
308
建立複合鑰匙
312
返回步驟 217

# 第七圖

## 元標記

1.IPMVERSION：以 n. n 主要、次要格式指的 ITF 格式版本號碼。範例爲<ITFVERSION>：0.1

2.ITFNEWFILE：此元標記表示新的方塊之元標記以及隨後之元資料。應爲跟隨 ITFVERSION 元標記之第一元標記。此元標記後設計成使得 ITF 檔案可用於 Batch 下載。

3.ITFFID：此標記保持此項目之資料 id。

4.ITFSERVER:指定至包含欲處理檔案之伺服器的 IP 鏈結。可爲 DNS 項目或 IP 號碼。較佳爲 IP 號碼，故吾人不需仰賴 DNS 轉譯。

5.ITFFILENAME：欲處理檔案之名稱。

6.ITFARTIST：歌曲演唱者。可爲以逗號界定的複合名字。

7.ITFTITLE：歌曲名稱。

8.ITFALBUB：歌曲所屬之專輯名稱。

9.ITFCOST：此標記包括項目之費用。

10.ITFDATE：產生資料檔或最後更新。Mm/dd/yy。

11.ITFSIZE：此標記包含項目的檔案大小。

使用規則：

1.所有元標記係以小於符號「＜」開始，而以冒號及大於符號「：＞」結束。

2.所有元標記必須開始於一行的第一列。

3.元資料立即跟隨元標記之結尾：＞，並以新的元標記或是檔案結尾而結束。此允許使用任何字母或包括字母的內文序列以用於界定元標記本身。注意，如果埋入的元標記在新的一行開始，不要嘗試將元標記埋在元資料內。